Lampi di Cassandra/ Fango contro Tails

(327)—Una PSYOPS contro Tails. Ovvero come si può lavorare contro l'anonimato, ribaltando i termini delle Public Disclosure.

Lampi di Cassandra/ Fango contro Tails

Figure 1:

(327)—Una PSYOPS contro Tails. Ovvero come si può lavorare contro l'anonimato, ribaltando i termini delle Public Disclosure.

Figure 2:

25 luglio 2014—Sulla quotata rivista di business *Forbes* è apparso un articolo molto ben scritto, che sostiene l'esistenza di vulnerabilità zero-day in Tails, e ne scoraggia, anzi ne sconsiglia in pratica l'uso.

Probabilmente esistono; i bug esistono in tutti i software, e non si vede perché software come Tor, I2P o distribuzioni GNU/Linux come Tails dovrebbero esserne esenti. Pare appunto, come sostengono varie fonti che trovate in questo post, che sia I2P il componente di Tails (oltretutto poco usato) che è bacato. Ma le conclusioni che si devono trarre da questa notizia sono totalmente contrarie a quelle istintive.

Usate Tails se non la usate, continuate ad usarla se la state usando, perché malgrado tutto attualmente non c'è niente di meglio per gli utenti normali della Rete. L'intera operazione magari non sarà una PSYOPS contro Tails, ma è indistinguibile da una PSYOPS: ecco perché.

Normalmente cosa succede quando qualcuno onesto individua una vulnerabilità in un software molto diffuso?

Succede che viene fatta una "responsible disclosure". Chi ha trovato il bug avverte non pubblicamente gli sviluppatori per dar loro il tempo di correggerlo.

Se gli sviluppatori dopo un tempo ragionevole non lo fanno, rende pubblico il bug in modo da massimizzare le probabilità che venga corretto.

Qui succede esattamente il contrario. Qualcuno che lavora per un cliente particolare trova un bug, ed invece di avvertire gli sviluppatori perché lo correggano, comunica pubblicamente l'esistenza del bug, e non il bug stesso. Il pubblico viene scoraggiato ad usare il software e gli sviluppatori non sono in grado di correggerlo. Nel frattempo, chi ha individuato il bug può utilizzarlo a piacere, e può farlo utilizzare da un ipotetico cliente che ipoteticamente gli avesse commissionato la ricerca.

L'articlo di *Forbes* afferma appunto che Exodus Intelligence, che ha trovato il bug e ne ha comunicato l'esistenza al mondo, non lo ha reso pubblico perché il suo cliente lo possa sfruttare.

C'è altro da aggiungere? No.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on July 20, 2023.

Canonical link

Exported from Medium on August 27, 2025.